

---

---

**CCEVS Workshop  
September 9, 1998**

**Introduction to the  
Common Criteria for IT Security  
&  
Common Evaluation Methodology**

**Gene Troy  
NIST**

# Goals of CC Project

---

- **Single (common) IT product / system security criteria**
  - based on prior criteria in North America and Europe
- **ISO standard criteria identical to CC**
- **Level international playing field for developers**
- **Mutual recognition of product evaluations**
- **Better availability of IT security-capable products**

# Common Criteria General Model

---

*The Common Criteria --*

*A well-understood / common / flexible  
technical basis for IT security:*

- **Describing IT product security requirements**
  - Protection Profile and Security Target (Part 1)
  - Catalog of security functional requirements (Part 2)
- **Evaluating IT product security features:**
  - Catalog of assurance requirements (Part 3), including...
  - Seven Evaluation Assurance Levels (EALs)

# **Key Concepts (1)**

## **Kinds of Requirements**

---

### **IT Security Requirements**

**-- Two kinds:**

#### **Functional Requirements**

- for defining security behavior of the IT product or system:
- implemented requirements become security functions

#### **Assurance Requirements**

- for establishing confidence in Security Functions:
- correctness of implementation
- effectiveness in satisfying objectives

# Key Concepts (2)

## -- The Constructs

---

- **Protection Profile (PP):**

An **implementation-independent** set of security objectives and requirements for a category of products or systems that meet similar consumer needs for IT security.

- ***Examples: Firewall-PP, C2-PP, RBAC-PP***

- **Security Target (ST):**

A set of security requirements and specifications for an **identified IT product** or system (a.k.a. “Target Of Evaluation”) -- to be used as the basis for its evaluation.

- *Example: ST for Oracle v7, ST for MilkyWay Firewall*

# Key Concepts (3)

## -- About the TOE

---

- **Target of Evaluation (TOE):**  
An IT product or system that is the **subject** of an evaluation.
- **TOE Security Policy (TSP):**  
The **rules** that regulate how assets are managed, protected and distributed within a TOE.
- **TOE Security Functions (TSF):**  
All parts of the TOE that must be **relied upon** for the correct enforcement of the TSP.

# Key Concepts (4)

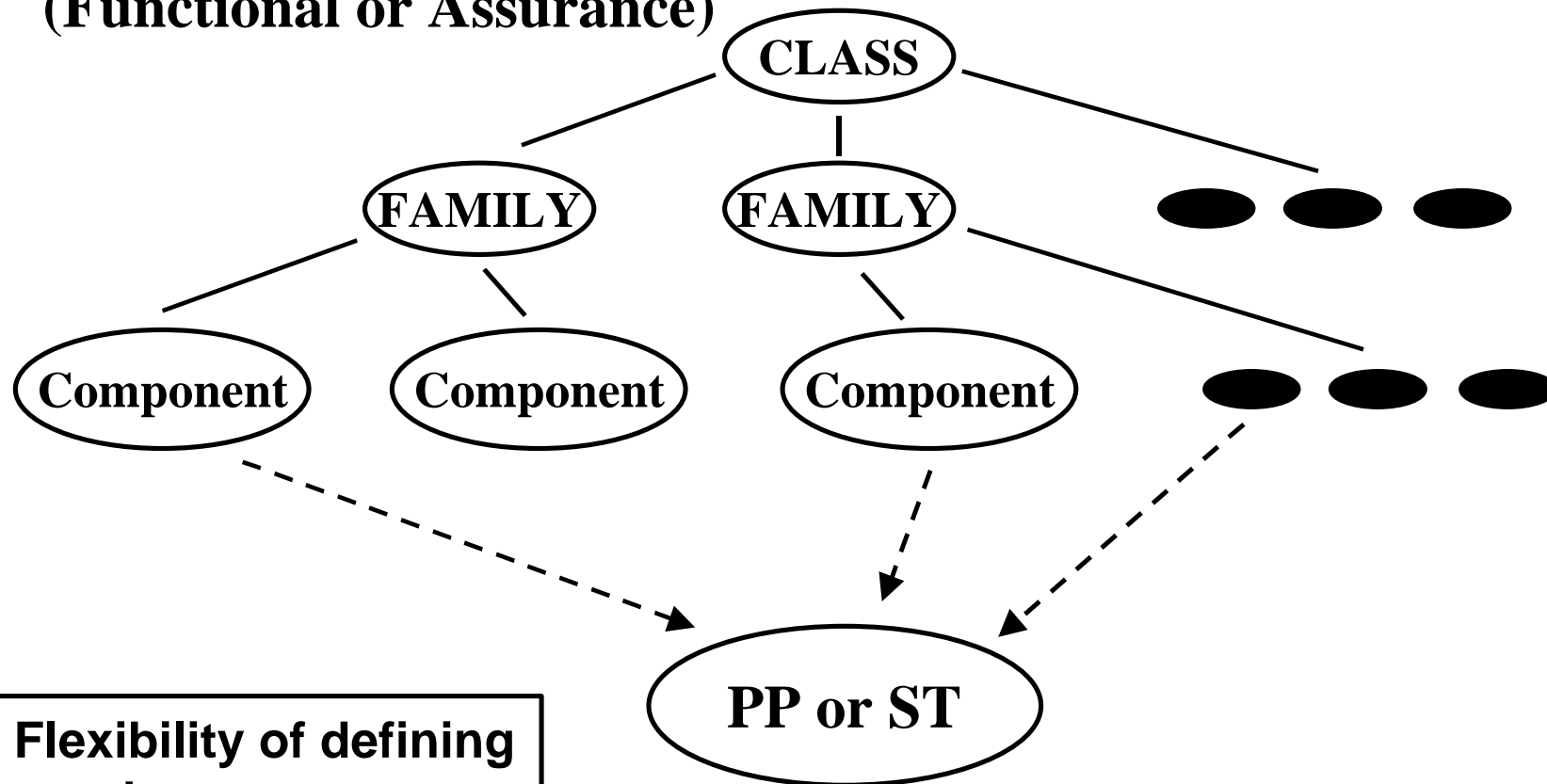
## Hierarchy of the Parts

---

- **CC functional / assurance hierarchy:**  
a set of constructs that classify security requirement components into related sets:
  - **Class (e.g. FDP - User Data Protection):**  
a grouping of **families** that share a common focus.
  - **Family (e.g. FDP\_ACC - Access Control Policy):**  
a grouping of **components** that share security objectives but may differ in emphasis or rigor.
  - **Component (e.g. FDP\_ACC.1 - Subset Access Control):**  
the smallest selectable set of **elements** that may be included in a PP / ST / package.

# Example Hierarchy

(Functional or Assurance)



Flexibility of defining requirements.

# Part 2 -- Security Functional Classes

---

## ➤ Classes of Security Functional Requirements:

<b>Class</b>	<b>Name</b>
<b>FAU</b>	<b>Audit</b>
<b>FCO</b>	<b>Communications</b>
<b>FCS</b>	<b>Cryptographic Support</b>
<b>FDP</b>	<b>User Data Protection</b>
<b>FIA</b>	<b>Identification &amp; Authentication</b>
<b>FMT</b>	<b>Security Management</b>
<b>FPR</b>	<b>Privacy</b>
<b>FPT</b>	<b>Protection of TOE Security Functions</b>
<b>FRU</b>	<b>Resource Utilization</b>
<b>FTA</b>	<b>TOE Access</b>
<b>FTP</b>	<b>Trusted Path / Channels</b>

# Part 3 -- Security Assurance Classes

---

## ➤ Classes of Security Assurance Requirements:

Class	Name
ACM	Configuration Management
ADO	Delivery & Operation
ADV	Development
AGD	Guidance Documents
ALC	Life Cycle Support
ATE	Tests
AVA	Vulnerability Assessment
▶ APE	Protection Profile Evaluation
ASE	Security Target Evaluation
▶ AMA	Maintenance of Assurance

# Evaluation Assurance Levels (EALs)

---

## ➤ Evaluation Assurance Levels & *(rough)* Backward Compatibility Comparison

<b>EAL</b>	<b>Name</b>	<b>*TCSEC</b>
<b>EAL1</b>	<b>Functionally Tested</b>	
<b>EAL2</b>	<b>Structurally Tested</b>	<b>C1</b>
<b>EAL3</b>	<b>Methodically Tested &amp; Checked</b>	<b>C2</b>
<b>EAL4</b>	<b>Methodically Designed, Tested &amp; Reviewed</b>	<b>B1</b>
<b>EAL5</b>	<b>Semiformally Designed &amp; Tested</b>	<b>B2</b>
<b>EAL6</b>	<b>Semiformally Verified Design &amp; Tested</b>	<b>B3</b>
<b>EAL7</b>	<b>Formally Verified Design &amp; Tested</b>	<b>A1</b>

\*TCSEC = “Trusted Computer Security Evaluation Criteria” --”Orange Book”

# Protection Profiles (generic) & Security Targets (specific)

---

## *Protection Profile contents*

- Introduction
- TOE Description
- Security Environment
  - Assumptions
  - Threats
  - Organizational Security Policies
- Security Objectives
- Security Requirements
  - Functional Req'ts
  - Assurance Req'ts
- Rationale

## *Security Target contents*

- Introduction
- TOE Description
- Security Environment
  - Assumptions
  - Threats
  - Organizational Security Policies
- Security Objectives
- Security Requirements
  - Functional Req'ts
  - Assurance Req'ts
- *TOE Summary Specification*
- *PP Claims*
- Rationale

# CC Evaluation

---

## **Types of Evaluation in CC:**

- **Protection Profile evaluation (Part 3 - APE)**
- **Product / system evaluation (two phases):**
  - **Security Target evaluation (Part 3 - ASE)**
  - **TOE evaluation (uses evaluated ST as baseline)**

# **Common Criteria**

## **-- Current Status**

---

### **➤ Current Version:**

- CC version 2.0, May 1998
- a.k.a. ISO Final Committee Draft (FCD) International Standard 15408
- Minor tweak expected this Fall (editorial/errata)

### **➤ Future Plans:**

- Upcoming ISO balloting for final International Standard 15408 -- expected completion: 2/99
- CC Interpretations Management Board (CCIMB) now established to interpret CC & maintain in future

# Common Evaluation Methodology

---

- **What is the Common Evaluation Methodology?**
  - A **companion** to the CC.
  - Focuses on **actions** evaluators must take to determine that CC requirements have been complied with.
  - Used by evaluation schemes to ensure **consistent application** of CC requirements across multiple evaluations and multiple schemes.
  - Therefore, an important component of **mutual recognition**.

# **CEM -- Approach & Contents**

---

- **Part 1: Introduction & General Model**
  - Terminology & principles of evaluation
- **Part 2: Evaluation Methodology**
  - PPs & STs (APE & ASE)
  - EALs 1-4
  - EALs 5-7
  - Other assurance components
- **Part 3: Extensions to Methodology (planned)**
  - Contents not decided yet

# CEM -- Release Schedule

---

- **Part 1: Introduction & General Model**
  - draft out for review (1/97)
- **Part 2: Evaluation Methodology**
  - PPs (APE): draft out for review (9/97)
  - STs (ASE) & EAL1-EAL4: draft expected out for review post-October 1998
  - EAL5-EAL7: no schedule yet
- **Part 3: Extensions to Methodology**
  - No schedule yet

(See NIST's CC website for draft CEM review postings --  
<http://csrc.nist.gov/cc/cem/cemlist.htm>)

# CC Contact Information

---

**To obtain a copy of the CC:**

**(PDF and Frame5 formats)**

- **<http://csrc.nist.gov/cc/ccv20/ccv2list.htm>**

**For further information on the CC, contact:**

- **Eugene F. (Gene) Troy**

**NIST/ITL**

**Building 820 (NIST North)**

**Gaithersburg, MD 20899, USA**

- **email: [eugene.troy@nist.gov](mailto:eugene.troy@nist.gov)**

**CC on web: <http://csrc.nist.gov/cc>**

**phone: (301) 975-3361**

**fax: (301) 926-2733**